

19-mj-1175-DLC

**AFFIDAVIT OF FBI SPECIAL AGENT BRYCE MONTOYA
IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Bryce Montoya, having been first duly sworn, do hereby depose and state as follows:

1. I have been employed as a Special Agent of the FBI since May 2018 and I am currently assigned to the Boston Division, Lakeville Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to, among other things, the online sexual exploitation of children. During my training at the FBI Academy, Quantico, Virginia, I received training in a variety of investigative matters.

2. The FBI Indianapolis Division is currently investigating Jeffrey LEBERT ("LEBERT") for offenses including 18 U.S.C. § 2251(a) and (e) - Use of Materials to Coerce a Minor to Engage in Sexually Explicit Conduct for the Purpose of Producing a Visual Depiction of Such Conduct and for the Purpose of Transmitting a Live Visual Depiction of Such Conduct; and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)- Possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography. On May 22, 2019, a federal grand jury in the Northern District of Indiana returned a one-count indictment charging LEBERT with one count of violating 18 U.S.C. § 2251(a) and (e) (Use of Materials to Coerce a Minor to Engage in Sexually Explicit Conduct for the Purpose of Producing a Visual Depiction of Such Conduct and for the Purpose of Transmitting a Live Visual Depiction of Such Conduct).

3. I am submitting this affidavit in support of an application for a search warrant to search a black Samsung mobile phone that was seized on May 28, 2019 incident to LEBERT's arrest (hereinafter "the TARGET CELLPHONE"). The TARGET CELLPHONE is more fully described in Attachment A to this affidavit.

4. For the reasons set forth below, I have probable cause to believe that the TARGET CELLPHONE contains data and records of contraband, evidence of a crime, fruits of a crime, and/or instrumentalities of the Target Offenses as set forth in Attachment B. Accordingly, I am requesting issuance of a search warrant for the TARGET CELLPHONE, as further described in Attachment A, authorizing the search and seizure of contraband, evidence, fruits of a crime, and/or instrumentalities the Target Offenses, as more fully described in Attachment B.

5. The statements contained in this affidavit are based in part on: written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of securing and authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

STATEMENT OF PROBABLE CAUSE

6. In February 2019, an FBI online covert employee (“OCE”) was connected to the Internet in an online undercover capacity. The OCE posted numerous online bulletin messages on specific social media forums which—based on the OCE’s training and experience and on information gathered from other sources—are websites frequented by individuals who have a

sexual interest in children. One such social media platform used by the OCE was Kik.¹ The OCE purported to have a 14-year-old step-daughter with whom he was sexually active.

7. On February 22, 2019, an individual using the Kik screen name “Ryan Jones” and Kik username “jonesryanfr” initiated a personal message with the OCE on Kik. During various online conversations, which took place between February 22, 2019 and March 3, 2019, “Ryan Jones” expressed interest in watching a live stream on Skype² of the OCE engaging in sexual activity with the OCE’s purported 14-year-old step-daughter. “Ryan Jones” did not have a Skype account and told the OCE that he would have to set one up. Once “Ryan Jones” established a Skype account, he told the OCE that his Skype username was “jlebert755 / Ryan Jones.” “Ryan Jones” also gave the OCE the email address “jlebert755@gmail.com.”

8. On March 2, 2019, “Ryan Jones” spoke with the OCE via Skype video. During this Skype video call, “Ryan Jones” admitted to having had a sexual relationship with a 14-year-old child when he was 28 years old. The OCE was able to see “Ryan Jones” clearly during the Skype video call. During the Skype video call, the OCE also noticed that the orientation of the camera used by “Ryan Jones” was in “portrait mode.” This is consistent with video commonly taken from wireless devices such as cellular telephones. “Ryan Jones” and the OCE made arrangements to have a Skype video call the next day. After the first Skype video call, “Ryan Jones” sent the OCE Kik messages such as:

- “I cant wait till tomorrow”

¹ Kik is a free instant messaging mobile application available on iOS- and Android-based smartphones. Kik uses a smartphone’s data plan or wireless Internet connection to transmit and receive messages, photos, videos, sketches, and mobile webpages.

² Skype is a telecommunications application that specializes in providing video chat and voice calls between computers, tablets, mobile devices, and other electronic devices. Skype is available for download on mobile phones, such as the TARGET CELLPHONE.

- “So did I make the cut? lol”
- “I wanna watch her suck ur cock nice and slowly and lick the tip and up and down the base.”
- “I want her to spit on ur cock and stroke it while she looks into the camera at me talking dirty.”

9. On March 3, 2019, “Ryan Jones” and the OCE had another Skype video call. Again, the face of “Ryan Jones” was clearly visible to the OCE. “Ryan Jones” told the OCE he wanted to see the OCE’s purported 14-year-old step-daughter’s “...pussy as she was getting fucked.” “Ryan Jones” also said that he wanted the OCE to ejaculate inside her vagina. After the OCE terminated the Skype video call, “Ryan Jones” messaged the OCE on Kik. “Ryan Jones” described in detail the specific sexual acts he wanted to see the OCE engage in via livestream on Skype with the OCE’s purported 14-year-old stepdaughter. For example, “Ryan Jones” told the OCE he wanted to:

- “see her sucking on the tip and stroking ur cock”
- “I wanna see her play with her pussy”
- “I wanna see u ravage her yung body but passionately”

Additionally, “Ryan Jones” asked:

- “She’s 14 rite? I cant remember 14 or 15”

10. On March 4, 2019, a subpoena was sent to Kik requesting identifying information for the screen name “Ryan Jones” with username “jonesryanfr.” On March 5, 2019, Kik complied with the subpoena and supplied the following information:

Subscriber: Ryan Jones
Email address: fallriv1982@gmail.com (confirmed)
Username: jonesryanfr
Registration: 2019/2/10 17:10:28
User Location: US (tz: America/New York, ip: 71.248.175.127.

11. Kik also provided the last 30 days of IP address activity for the account. Some of the IP addresses associated with the Kik account at or around the time of the Kik communications between the OCE and “Ryan Jones” were assigned to a mobile network provider. Additional IP addresses captured around the time “Ryan Jones” communicated on Kik with the OCE were assigned to a business in the Kingston Collection shopping mall in Kingston, Massachusetts (“Business 1”). Kik also provided information that the username “jonesryanfr” installed the Kik mobile application on a Samsung device with Android software on or about February 10, 2019. Based upon this information and my own training and experience, I believe that the individual claiming to be “Ryan Jones” was using the Kik application on a cellular telephone or similar communication device.

12. Based on information provided to the OCE by “Ryan Jones” (*e.g.*, the Skype user name “jlebert755 / Ryan Jones” and the email address jlebert755@gmail.com), an FBI Special Agent searched publicly-available information for “Lebert” in Fall River, Massachusetts. The FBI Special Agent located records for a “Jeffery Alan Lebert” (LEBERT) with a residential address in Plymouth, Massachusetts. Additionally, the FBI Special Agent located a Facebook account under the name “Jeffrey Lebert.” The Facebook account indicated that “Jeffrey Lebert” was from Fall River, Massachusetts, which is consistent with the “fr” in “Ryan Jones’s” Kik username “jonesryanfr” and with the confirmed email address provided by Kik for “Ryan Jones” (fallriv1982@gmail.com).

13. The FBI Special Agent in Indianapolis located a Massachusetts identification card for LEBERT. According to that Agent, the person in LEBERT’s identification card photograph, the person in the Kik social media account, and Skype user “Ryan Jones” all appear to be the same person. Special Agents in Indianapolis also believe that the Facebook post containing a picture of

LEBERT is the same photograph used as the contact photograph for the Skype account of “Ryan Jones.”

14. On May 16, 2019, an FBI Special Agent and I conducting surveillance observed LEBERT working at a business in the Kingston Collection shopping mall (“Business 2”) in Kingston, Massachusetts. LEBERT appeared to be holding a cellular telephone. I believe based upon this surveillance that an individual inside Business 2 would likely be within range to connect to the wireless internet belonging to Business 1. While conducting surveillance, I also determined that the internet service belonging to Business 1 did not require a password to access the network. Based on this information, as well as my training and experience, I believe that LEBERT accessed his Kik account using a cellular telephone connected to Business 1’s unsecured wireless internet.

15. On May 28, 2019, other law enforcement officers and I arrested LEBERT pursuant to an arrest warrant issued in the Northern District of Indiana. At the time of his arrest, the TARGET CELLPHONE was on LEBERT’s person and was seized incident to his arrest. After being advised of his *Miranda* rights and initially agreeing to answer questions, LEBERT subsequently asked to speak with a lawyer.

**PRODUCTION OF CHILD PORNOGRAPHY
AND THE POSSESSION OF CHILD PORNOGRAPHY**

16. Based on my training and experience, I know individuals involved in the production of child pornography often store pornographic images and videos for their personal review. These explicit images are capable of being stored on digital devices, including but not limited to cellular telephones. Additionally, individuals involved in the production of child pornography often keep pornographic images for distribution; particularly to trade with other individuals involved in the exploitation of children. In the modern age, this trading is often done via the Internet, and through mobile applications including but not limited to Kik and Skype. Because LEBERT is suspected

to be involved in the production of child pornography, I believe that the TARGET CELLPHONE may contain images and/or videos of child pornography.

**CHARACTERISTICS COMMON TO CONSUMERS OF CHILD
PORNOGRAPHY**

17. Based on my previous investigative training and experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who consume child pornography:

- a. Consumers of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Consumers of child pornography may collect sexually explicit or suggestive materials, in a variety of visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Consumers of child pornography often maintain their collections in a digital or electronic format in a safe, secure and private environment, such as a computer or cell phone. These collections are often maintained for several years and are kept close by, to enable the individual to view the collection, which is valued highly.

- d. Consumers of child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- e. Consumers of child pornography prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- f. These offenders obtain and/or traffic in materials depicting children engaged in sexually explicit conduct through many sources and by several methods and means. These sources, methods, and means include but are not limited to downloading via the Internet and other computer networks (such as web sites, peer-to peer file sharing networks, electronic bulletin boards, chat rooms, instant message conversations, e-mail, and mobile applications such as Kik and Skype), trading with other persons with similar interests through such electronic transfer, and producing and manufacturing these materials during actual contact with children or manipulating children into creating such materials and providing them to the perpetrator.

18. Based upon the foregoing, there is probable cause to believe that LEBERT, as the user of the TARGET CELLPHONE, displays characteristics common to individuals who consume child pornography. Based on my knowledge, training, and experience, I am aware that the records and data as set forth in Attachment B, relating to individuals engaged in the production,

distribution, and receipt of child pornography have been recovered from the search of smartphones used by individuals engaged in such activities, and that such records and data constitute evidence of the Target Offenses. As such and given the facts of this investigation, I believe that there is probable cause to believe that the TARGET CELLPHONE will contain evidence of the Target Offenses, contraband, the fruits of the Target Offenses, and/or property designed or intended for use or which is or has been used as the means of committing the Target Offenses as set forth in Attachment B.

MOBILE COMMUNICATION DEVICES

19. I know from my training and experience that modern digital devices such as cellular telephones, tablets, and other communication devices are extremely portable. With the advancements in processing power and storage capacity, many of these devices operate similar to stand alone “desktop” type computers. Application developments, communication capabilities and portability have made these devices an indispensable part of everyday life. Persons who have these devices, particularly cellular telephone type platforms, typically keep them on their persons or in other readily available locations. I believe that the inherent portability of modern digital devices combined with evidence to believe LEBERT accessed his Kik and Skype accounts on a mobile device from multiple locations give probable cause to believe that the items referenced in Attachment B will be located on the TARGET CELLPHONE.

SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND DATA

20. As set forth above, I believe that there is probable cause to believe that LEBERT used the TARGET CELLPHONE in connection with the Target Offenses, and that evidence of the Target Offenses will be found on the TARGET CELLPHONE.

21. The TARGET CELLPHONE is a smartphone. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, accessing the internet, and storing a vast range and amount of electronic data. In many respects, a smartphone shares many of the capabilities and functions of a computer. Based upon my knowledge, training and experience, I know that a cellular telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Based on my training and experience, I know that the TARGET CELLPHONE has all of these capabilities.

22. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers or cellphones, they can easily transfer the data from an old computer or cellphone to a new computer or cellphone.
- b. Even after files have been deleted, those files can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

23. Based upon the foregoing, I have probable cause to believe that a review of the TARGET CELLPHONE for the items listed above and described in Attachment B will result in the seizure of evidence, fruits and instrumentalities of the Target Offenses.

NATURE OF EXAMINATION

24. Based on the foregoing, and consistent with Rule 41 of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the TARGET CELLPHONE. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many digital electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

26. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Most devices offer a feature that allow the user to store a finite number of fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's fingerprint sensor. The location of the fingerprint sensor may vary depending on the model of device.

27. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain

Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple’s “Face ID”) have different names but operate similarly to Trusted Face.

28. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

29. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

30. The passcode or password that would unlock the device subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not

otherwise be able to access the data contained within the communication device, making the use of biometric features necessary to the execution of the search authorized by this warrant.


31. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

32. As a result, I am also seeking authorization from this Court in the requested search warrant allowing me to obtain from LEBERT the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the TARGET CELLPHONE in order to conduct the proposed search, including to (1) press or swipe LEBERT's fingers (including thumbs) to the fingerprint scanner of the TARGET CELLPHONE; (2) hold the TARGET CELLPHONE in front of his face to activate the facial recognition feature; and/or (3) hold the TARGET CELLPHONE in front of LEBERT's face to activate the iris recognition feature.

CONCLUSION


33. Based on the foregoing, there is probable cause to believe that LEBERT has engaged in conduct in violation of the Target Offenses, and that contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located within the TARGET CELLPHONE, described in Attachment A. I respectfully request that this Court issue a search warrant for the TARGET CELLPHONE authorizing the seizure and search of the items described in Attachment B.

34. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered and a description of the physical storage media that was seized or copied. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.



Bryce Montoya
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 28th day of May 2019.



Honorable Donald L. Cabell
United States Magistrate Judge
District of Massachusetts



ATTACHMENT A

(Property to be Searched)

TARGET CELLPHONE: A black Samsung cell phone that was seized from Jeffrey LEBERT incident to his arrest on May 28, 2019, and which is currently in the possession of the FBI.

ATTACHMENT B

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations and attempted violations of 18 U.S.C. §§ 2251 (a) and (e) (Use of Materials to Coerce a Minor to Engage in Sexually Explicit Conduct for the Purpose of Producing a Visual Depiction of Such Conduct and for the Purpose of Transmitting a Live Visual Depiction of Such Conduct) and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography):

- a. Electronically stored telephone numbers, names, addresses, or other directory information identifying directory or contact telephone numbers with individual users.
- b. Stored photographs or videos, including all metadata associated with any stored photographs and videos;
- c. Any and all information regarding the telephone call number or other associated identifying numbers.
- d. Information regarding incoming or outgoing calls.
- e. GPS or other location information.
- f. Stored or deleted text messages, emails, instant messages, chat and/or electronic communications, including but not limited to messages sent and received from the Kik and Skype mobile applications.
- g. Identifying numbers such as, but not limited to, the device(s)' International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI) number, and Android ID number.
- h. Internet searches or other online inquiries or applications or software downloads, and any other information or data, including deleted data.
- i. Information related to the existence of applications present on the device(s), or information related to the former existence of applications on the phone, including, but not limited to, functions of the applications, dates and times downloaded and frequency of use.
- j. Evidence of user attribution showing who used or owned the device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

2. Records evidencing the use of the Internet Protocol address[es] associated with the device(s) including:

- a. Records of Internet Protocol addresses used;
- b. Records of Internet activity, including firewall logs, caches, Internet networks used, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

During the execution of the search of the Target Cellphone described in this warrant in Attachment A, law enforcement personnel are authorized to obtain from Jeffrey LEBERT the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the TARGET CELLPHONE in order to conduct the proposed search, including to (1) press or swipe Jeffrey LEBERT's fingers (including thumbs) to the fingerprint scanner of the TARGET CELLPHONE; (2) hold the TARGET CELLPHONE in front of Jeffrey LEBERT's face to activate the facial recognition feature; and/or (3) hold the TARGET CELLPHONE in front of Jeffrey LEBERT's face to activate the iris recognition feature.

DEFINITIONS

For the purpose of this warrant:

- A. "Equipment" means any hardware, software, storage media, and data.
- B. "Hardware" means any electronic device capable of data processing (such as a computer, digital camera, cellular telephone or smartphone, wireless communication device, or GPS navigation device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related

communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

- C. "Software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security
- D. software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, USB or thumb drive, or memory card).
- F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.
- G. "Record(s)" is any communication, representation, information or data.